COPIA FINANCIAL SOLUTIONS, INC.

An *Objective* Approach to Comprehensive Wealth Management

Steps to Take: Fraud Protection/Cyber Security

The recommendations below can reduce the risks of cyber fraud and identity theft.

- Consider placing a Credit Freeze at ALL 3 agencies to restrict access to your credit report. Restricting access to your credit report makes it harder for identity thieves to open new accounts in your name, since most creditors need to see your credit report before approving a new account -- without your file, they will generally be unwilling to extend the credit. As of September of 2018, placing or removing a freeze is free, and the credit agencies are mandated to place or remove a freeze within 1 hour if properly done online or by phone https://www.consumer.ftc.gov/blog/2018/09/free-credit-freezes-are-here..

  - **Equifax** https://www.equifax.com/personal/credit-report-services/ or 1-800-349-9960
  - **Experian** https://www.experian.com/freeze/center.html or 1-888-397-3742
  - **TransUnion** https://www.transunion.com/credit-freeze or 1-888-909-8872

- Order credit reports from all 3 agencies annually, a FREE service at www.annualcreditreport.com, and look for any unauthorized accounts or "hard inquiries", or negative activity (late payments, collection activity, liens or defaults).

- Protect minors' from identity theft. As of September 2018, **federal law** made it easier for families to combat this growing problem of identity fraud, allowing them to make inquiries about credit files in their child's name and freeze a file at no cost. Go to **https://identitytheft.gov/Steps**, scroll down and click on the Child Identity Theft section, under Special Forms of Identity Theft, then view instructions on how to find out if your child has a credit report. Most young children shouldn't have credit files. Some experts recommend parents create a credit file for their children and freeze it. If you do this, keep the record of freezes in a safe place, so the child or a guardian can find it when needed.

- Review credit card and bank statements monthly, and consider email or text notices of transactions. With the amount of activity we now routinely assign to credit cards, whether in person or online, it can be challenging keeping up with the oversight. This (as well as the benefits of consolidating "points" and other benefits) may argue for limiting the number of credit cards you maintain, and formally closing infrequently used accounts.

- Similarly, review claim statements from your health insurance provider for fraudulent claims. You may also wish to request a copy of your Medical Information Bureau ("MIB") report at http://www.mib.com/request_your_record.html (free, annually).

1063 West Hunting Drive Palatine, Illinois 60067
Tel 847-776-PLAN (7526) Fax 847-776-0455

COPIA FINANCIAL SOLUTIONS, INC.

An *Objective* Approach to Comprehensive Wealth Management

Steps to Take: Fraud Protection/Cyber Security

- Consider authorizing 2 factor authentication on online banking and other sensitive accounts, which requires a code (sent to a cell, home phone or email) for access.

- Few of us use wire transfer (ACH is the more common means of electronic transfer). To protect yourself from unauthorized wire transfers, you may be able to simply "turn off" this service at your bank.

- When using apps or visiting sensitive sites that contain personal information (especially financial sites and social media) be sure use strong passwords *https://www.wikihow.tech/Create-a-Secure-Password*, and avoid the temptation to use the same password for multiple sites. If maintaining a lot of different passwords is an unrealistic burden, consider a password manager (see http://thewirecutter.com/blog/password-managers-are-for-everyone-including-you/ or http://www.pcmag.com/article2/0,2817,2407168,00.asp).

- Consider enrolling in a credit monitoring/ID Theft Protection service. None of these guarantee that you are 100% protected from identity theft. They do advertise a number of services designed to identify threats and suspicious activity, and assist with, and reimburse for the cost of, identity restoration. Offered by the 3 credit agencies as well as other firms, the services can include data breach detection, which involves aggregating data from online sources (known as "dark web forums") commonly used by criminals to buy and sell hacked data. Firms access these sites, and use information found there to warn consumers if, for instance, their email has been hacked, or some of their credit card info is on one of these forums.

- "Malware" has made its way around the globe, disrupting computer systems worldwide. Take action to ensure that especially your Windows-based systems are protected. Make it a practice to download and install all system updates from Microsoft and any other software vendors you use, and make sure your anti-virus protection is current and that your firewall is enabled. Visit Microsoft's website (https://support.microsoft.com/en-us/help/12373/windows-update-faq) and click "show all" for more information. And never open an email or attachment that you are not certain is from a safe source.

- Phone scams have become increasingly popular with criminals. Remember: neither the IRS nor the Social Security Administration make demands for payment or request credit card, bank account, social security or any other sensitive data by telephone. When in doubt, hang up. https://www.usa.gov/common-scams-frauds#item-37207

1063 West Hunting Drive Palatine, Illinois 60067
Tel 847-776-PLAN (7526) Fax 847-776-0455